

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж



ЗАТВЕРДЖУЮ

Декан ФПКТС

Савенко О.С.

2020 р.

СИЛАБУС

Навчальна дисципліна: **Теорія передачі і захисту даних**

Освітньо-професійна програма: **Кібербезпека**

Рівень вищої освіти: **перший (бакалаврський)**

Загальна інформація

Позиція	Зміст інформації
Викладач	Орленко Вікторія Сергіївна
Профайл викладача	http://ksm.khnu.km.ua/sklad-kafedry/
E-mail викладача(ів)	Надається за домовленістю
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=5961
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/8577265687 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2020-2021, семестр III (осінньо-зимовий)
Розклад занять	Лекції: понеділок (чисельник), 5 пара, 1-2096 Практичні заняття: понеділок, 4 пара, 1-2096
Консультації	Очні: середа, 5 пара, 1-106 Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, у т.ч. ІРС			Залік	Іспит
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття						
Д	2	3	5,0	150	51	17	-	34	-	99	-	-	+	-

Анотація дисципліни

Дисципліна „Теорія передачі і захисту даних” складова професійної підготовки бакалаврів зі спеціальності „Кібербезпека”, є однією зі спеціальних профільюючих дисциплін.

Дисципліна викладається для студентів денної форми навчання спеціальності «Кібербезпека». При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні та репродуктивні, інтерактивні та ігрові, застосування інформаційно-комп'ютерних технологій.

Пререквізити: вища математика; дискретна математика.

Кореквізити: захист інформації в інформаційно-комунікаційних системах; прикладна криптологія.

Мета і завдання дисципліни

Дисципліна „Теорія передачі і захисту даних” – вибіркова складова професійної підготовки бакалаврів спеціальності “125 – Кібербезпека”.

Мета дисципліни. Полягає у поглибленні знання та розуміння предметної області щодо процесів передачі і захисту даних в інформаційно-телекомунікаційних (автоматизованих) системах на каналному рівні, способів оцінки та забезпечення ефективності і надійності функціонування систем передачі даних, методів оптимального та завадостійкого кодування даних та їх ролі в задачах криптографічного захисту

Предмет дисципліни. Методи визначення і контролю показників кількості і якості інформації, способи передачі і захисту даних, види і характеристики інформаційних сигналів та каналів зв'язку, методи оптимального та завадостійкого кодування.

Завдання дисципліни. Забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності „Кібербезпека”:

компетентності:

КЗ 01. Здатність застосовувати знання у практичних ситуаціях.

КЗ 02. Знання та розуміння предметної області та розуміння професії.

КФ 02. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 05. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

результати навчання:

РН 05. Адаптуватися в умовах частотої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

РН 06. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

РН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

Студент, який успішно завершив вивчення дисципліни, повинен: *знати* зміст, задачі і методи теорії інформації, кодування та передачі даних; *застосовувати* знання у практичних ситуаціях, *адаптуватися* на їх основі в умовах частотої зміни технологій професійної діяльності, *прогнозувати* кінцевий результат; *використовувати* розуміння характеристик процесів передачі даних для виконання моніторингу процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки, зокрема, *щоб виявляти* небезпечні сигнали технічних засобів; *бути здатним* до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки в системах передачі даних і *застосовувати* теорії та методи захисту (перетворення сигналів, оптимальне та завадостійке кодування даних тощо) для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; *бути*

здатним забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної, в тому числі *вирішувати* задачі захисту (кодуванням, модулюванням тощо) потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; *демонструвати* знання та розуміння предметної області дисципліни та розуміння професії та *критично осмислювати* основні теорії, принципи, методи і поняття у навчанні та професійній діяльності, в тому числі базуючись на постулатах теорії інформації.

Тематичний і календарний план вивчення дисципліни

Номер тижня	Номер теми	Тема лекції*	Тема практичного заняття**	Самостійна робота студента		
				Зміст	Години	Література
1	2	3	4	5	6	7
1	1	Введення в дисципліну Інформація, дані і сигнали як об'єкт захисту. Теорії інформації, кодування, передачі і захисту даних як інструмент дисципліни. Введення в інформаційні системи, системи передачі і захисту даних. Геометричні моделі сигналу, завади і системи зв'язку	ПЗ1. Примітивне кодування цифрових даних в системах числення з довільною основою	Опрацювання теоретичного матеріалу, підготовка до ПЗ №1	5	[1] с. 6-11; [2] с.5-10, 88-105; [4] с.6-9; [5] с.24-30
2	1		ПЗ2. Примітивне стандартизоване кодування символічних даних	Опрацювання теоретичного матеріалу, підготовка до ПЗ №2	7	[1] с.5-15
3	1	Кількісна оцінка інформації. Ентропія Постановка задачі вимірювання кількості інформації. Структурні міри інформації. Адитивна логарифмічна міра Хартлі. Адитивна міра в структурному представленні. Імовірність та інформація. Кількість інформації в повідомленні системи з різними імовірностями станів. Введення в ентропію. Ентропія об'єднаних систем, умовна ентропія. Визначення взаємозв'язку ентропії та кількості інформації. Ентропія і надлишковість	ПЗ3. Математичні основи теорії інформації та кодування	Опрацювання теоретичного матеріалу, підготовка до ПЗ №3	5	[1] с. 16-32; [2] с.11-16; [4] с.9-11; [7] с.9-24
4	1		ПЗ4. Кількісна оцінка інформації та ентропія у системах з рівномірним розподілом ймовірностей	Опрацювання теоретичного матеріалу, підготовка до ПЗ №4	6	[1] с.16-22; [2] с.11-15; [3] с.6-18
5	1	Дискретні і безперервні повідомлення і сигнали. Цифрова обробка сигналів Дискретні і безперервні повідомлення. Теорема Котельникова. Квантування сигналів. Кодова імпульсна модуляція. Основні технічні характеристики каналів передачі сигналів. Швидкість передачі дискретних сигналів і її залежність від характеристик каналу. Теорема Найквіста. Дискретне перетворення Фур'є. Швидке	ПЗ5. Кількісна оцінка інформації та ентропія у системах з нерівномірним розподілом ймовірностей	Опрацювання теоретичного матеріалу, підготовка до ПЗ №5	5	[1] с. 11-15; [2] с.57-62; [5] с.39-41 [3] с.18-23

		перетворення Фур'є.				
6	2		ПЗ6. Умовна та взаємна ентропія	Опрацювання теоретичного матеріалу, підготовка до ПЗ №6	7	[3] с.23-44
7	2	Ентропія безперервних розподілів, передача безперервних повідомлень Ентропія безперервних розподілів. Основні властивості ентропії безперервних розподілів. Пропускна здатність каналу при передачі безперервних сигналів	Контрольна робота	Опрацювання теоретичного матеріалу, підготовка до КР	5	[2] с.29-32; [7] с.30-45
8	2		ПЗ7. Оцінка недовантаження та надлишковості кодованих повідомлень	Опрацювання теоретичного матеріалу, підготовка до ПЗ №7	7	[1] с.51-59; [3] с.23-32
9	2	Канал для передачі дискретних повідомлень за відсутності завад і ефективне (оптимальне) кодування Пропускна здатність дискретного каналу зв'язку без завад. Теорема Найквіста. Теоретико-математичні основи оптимального кодування. Перша теорема Клода Шеннона. Оптимальне кодування і стиснення (архівування) даних. Оптимальні нерівномірні коди Шеннона-Фано. Оптимальне нерівномірне кодування Хаффмена. Арифметичне ентропійне кодування. Словникові і потокові методи стиснення даних. Альтернативні методи стиснення даних. Оптимальне кодування і захист даних	ПЗ8. Оптимальне кодування повідомлень – коди Шеннона–Фано	Опрацювання теоретичного матеріалу, підготовка до ПЗ №8	5	[1] с. 51-69; [2] с.75-87, 95-96; [4] с.18-45; [5] с.64-69 ; [7] с.24-27; [3] с.32-47
10	2		ПЗ9. Оптимальне кодування повідомлень – коди Хаффмена	Опрацювання теоретичного матеріалу, підготовка до ПЗ №9	6	[1] с.51-59; [3] с.32-47
11	2	Канал для передачі дискретних повідомлень за наявності завад і завадостійке (надлишкове) кодування Пропускна здатність дискретного каналу за наявності завад. Теорема Шеннона для дискретного каналу з завадами (друга теорема Шеннона). Потенційна завадостійкість згідно з Котельниковим. Загальні принципи побудови завадостійких кодів. Теорема Шеннона для дискретного каналу з перешкодами. Принципи використання надлишковості для виявлення і виправлення помилок Кодова відстань. Зв'язок коригувальної здатності коду з кодовою відстанню. Завадостійкі коди та достовірність передачі даних	ПЗ10. Оптимальне кодування повідомлень - формування пакетів службових даних для передачі кодованих повідомлень	Опрацювання теоретичного матеріалу, підготовка до ПЗ №10	5	[1] с.33-44, 70-79; [2] с.72-74; [4] с.46-59; [5] с.70-79; [6] с.10-61; [7] с.28-30; [3] с.32-47
12	2		ПЗ11. Омнофонне та	Опрацювання	7	[3] с.32-47;

			ентропійне кодування як засіб рандомізації повідомлень і підвищення криптостійкості шифрів	теоретичного матеріалу, підготовка до ПЗ №11		[4]
13	2	Блокові завадостійкі корегуючі коди Геометрична інтерпретація блокових корегуючих кодів. Принципи побудови групових завадостійких кодів. Код Хеммінга і його використання для виправлення одиночної помилки. Методи автоматичного виявлення помилок	ПЗ12. Основи завадостійкого кодування	Опрацювання теоретичного матеріалу, підготовка до ПЗ №12	5	[1] с.70-83; [2] с.59-62; [7] с.47-55; [3] с.48-54
14	2		ПЗ13. Паритетні коди. Кодування за парністю та непарністю повідомлень і блоків даних	Опрацювання теоретичного матеріалу, підготовка до ПЗ №13	7	[1] с.70-79; [2] с.72-73; [3] с.55-61
15	3	Циклічні коди Загальні поняття і визначення Принципи побудови циклічних кодів Використання циклічних кодів для виявлення і коректування помилок	ПЗ14. Коди Хеммінга	Опрацювання теоретичного матеріалу, підготовка до ПЗ №14	5	[1] с.84-92; [2] с.62-65; [7] с.56-66
16	3		ПЗ15. Циклічні коди	Опрацювання теоретичного матеріалу, підготовка до ПЗ №15	7	[1] с.84-92; [3] с.65-72
17	3	Модуляція сигналів при передачі двійково-кодованих даних Модуляція як невід’ємна складова безпечної передачі даних Передача двійкових даних методом амплітудної модуляції (КІМ-АМ) Передача двійкових даних методом частотної модуляції (КІМ-ЧМ) Передача двійкових даних методом фазової модуляції. (КІМ-ФМ) Структура системи передачі даних із застосуванням модуляції Приклади застосування модуляції Завадостійкість різних методів прийому двійкових модульованих сигналів	Підсумкова контрольна робота	Опрацювання теоретичного матеріалу, підготовка до підсумкової КР	4	[2] с.45-46; [5] с.6-23; [6] с.10-17; [7] с.74-77

Умовні позначення: ПЗ – практичне заняття, КР – контрольна робота

* лекції проводяться раз у два тижні по 2 години;

** практичні заняття проводяться щотижня по 2 години.

Політика дисципліни

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і практичні заняття згідно з розкладом, не запізнюватися на заняття, контрольні точки виконувати відповідно до графіка. Пропущене практичне заняття студент зобов'язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До практичних занять студент має підготуватися за відповідною темою і проявляти активність. Набутті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ <https://www.khnu.km.ua/root/files/01/10/03/006.pdf>.

Оцінювання результатів навчання студентів

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів у семестрі за ваговими коефіцієнтами

Аудиторна робота		Контрольні заходи		Підсумковий контрольний захід
Вид заняття	Практичні заняття (мінімальна кількість оцінок - 5)	Контрольна робота 1	Контрольна робота 2	Залік за рейтингом
Тема	1-3	1	2	
Ваговий коефіцієнт	0,5	0,2	0,3	

Оцінювання практичних занять. Оцінка, яка виставляється за практичне заняття, складається з таких елементів: здатність обрати вірний підхід до розв'язування задач і обґрунтувати зроблений вибір; правильність та самостійність розв'язування задач, якість отримуваних результатів; вільне володіння студентом спеціальною термінологією і застосовуваними методами дисципліни, здатність критично осмислювати основні теорії, принципи, методи і поняття; уміння обґрунтувати прийняті рішення.

Оцінку, отриману на практичному занятті, викладач оголошує студенту одразу після його відповіді і проставляє в електронний журнал дисципліни.

Впродовж семестру студент має отримати на практичних заняттях щонайменше п'ять позитивних оцінок, щоб виконати програму дисципліни.

Оцінювання контрольної роботи. Контрольна робота передбачає для кожного студента виконання варіанту завдання, що складається з трьох задач..

Оцінювання контрольної роботи здійснюється за чотирибальною шкалою:

– оцінка відмінно ставиться, якщо студент правильно розв'язав всі задачі контрольної роботи, розв'язок задач супроводжується логічно викладеними поясненнями та обґрунтуваннями. У роботі допустимі дві-три несуттєві похибки, що не впливають на якість отриманих схемних рішень;

– оцінка добре ставиться, якщо студент правильно розв'язав всі задачі контрольної роботи, розв'язок задач супроводжується поясненнями, але логіка пояснень в роботі та їх обґрунтування є недостатніми або розв'язки задач отримано нераціональним методом. У роботі також допустимі дві-три несуттєві похибки, що не впливають на якість отриманих схемних рішень;

– оцінка задовільно ставиться, якщо студент загалом правильно розв'язав всі задачі контрольної роботи, але представив розв'язки задач без необхідних пояснень і обґрунтувань або допустив одну-дві помилки в обчисленнях;

– оцінка незадовільно ставиться, якщо студент не розв'язав (частково або повністю) хоча б одну задачу контрольної роботи або в ході отримання розв'язку припустився суттєвої помилки (помилки), що зумовило одержання хибних результатів.

Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями оцінювання знань.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	Узагальнений критерій
1	2
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві-три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка „задовільно”.

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Залік вважається зданим при отриманні студентом за зведеними результатами поточного контролю підсумкової оцінки з дисципліни від 3,00 до 5,00 балів. При цьому за вітчизняною шкалою ставиться оцінка за двобальною шкалою, а за шкалою ECTS – оцінка, що відповідає набраній студентом кількості балів.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ECTS встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	Інституційна інтервальна шкала балів	Інституційна оцінка, критерії оцінювання		
A	4,75–5,00	5	Зараховано	Відмінно – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4		Добре – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4		Добре – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3		Задовільно – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3		Задовільно – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	Незараховано	Незадовільно – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2		Незадовільно – необхідна серйозна подальша робота і повторне вивчення дисципліни

Питання для самоконтролю здобутих студентами результатів навчання

1. Предмет теорії інформації. Основні поняття та визначення теорії інформації. (Алфавіт. Повідомлення. Невизначеність апіорна та апостеріорна. Особливості сприйняття інформації в теорії інформації.)
2. Класифікація повідомлень за вміщеною інформацією. (Інформаційні шуми, інформація, дезінформація.)
3. Визначення та основні задачі теорії інформації, методи вирішення основних задач.
4. Поняття та основні задачі теорії кодування, методи вирішення основних задач. Рівномірні та нерівномірні коди.
5. Узагальнена структура інформаційної системи. Принцип дії.
6. Структура системи передачі інформації. Принцип дії. Класифікація каналів зв'язку.
7. Основні характеристики сигналів. Умова узгодженості сигналів з каналом зв'язку.
8. Модулювання сигналів. Поняття та мета модулювання.
9. Передача двійкових сигналів методом амплітудного модулювання.
10. Передача двійкових сигналів методом частотного модулювання.
11. Передача двійкових сигналів методом фазового модулювання.
12. Мультиплексування сигналів: поняття, види та принципи.
13. Класифікація сигналів: дискретні та безперервні, детерміновані та випадкові.
14. Елементарні детерміновані сигнали. (Класифікація. Одиначна функція Дирака. Ідеальний одиначний імпульс.)
15. Теорема Котельникова. (Теорема відліків)
16. Квантування сигналів. (Класифікація. Принципи квантування за рівнем, за часом, комбіноване)
17. Аналогові та цифрові сигнали. Принципи аналого-цифрового та цифро-аналогового перетворення сигналів.
18. Дискретне перетворення Фур'є. Швидке перетворення Фур'є.
19. Відповідність мір інформації напрямкам теорії інформації (структурному, статистичному та семантичному). Структурні міри інформації: класифікація.
20. Геометрична міра інформації.
21. Комбінаторна міра інформації.
22. Адитивна міра Хартлі.
23. Кількісна оцінка інформації (в т.ч. за умови наявності завад та вихід на початкову формулу за умови їх відсутності)
24. Поняття та властивості безумовної ентропії. (Поняття повних систем подій. Формули для різних/однакових імовірностей. 5 властивостей).
25. Ентропія та надлишковість. Поняття недовантаженості та надлишковості. (Причини виникнення. Корисні властивості. Формули).
26. Канал для передачі дискретних повідомлень за умови відсутності завад. Основні визначення. (Середня швидкість передачі повідомлень. Швидкість передачі повідомлень. Пропускна здатність. Основна та три складових задачі дослідження зазначених каналів.)
27. Пропускна здатність дискретного каналу за умови відсутності завад. (Формула. Умова максимального використання.)
28. Теорема Шеннона для оптимального кодування.
29. Канал для передачі дискретних повідомлень за умови наявності завад. Особливості впливу завад на передачу повідомлень.
30. Пропускна здатність дискретного каналу за умови наявності завад.
31. Теорема Шеннона для дискретного каналу за умови наявності завад. (Наслідки, приклади, висновки).
32. Надлишковість інформації. Семантична та статистична надлишковість.
33. Оптимальне кодування: визначення; властивості; принципи.
34. Побудова оптимального коду за методом Шеннона-Фано.
35. Оптимальне кодування Хафмена.
36. Завадостійке кодування: основні поняття та загальні принципи побудови завадостійких кодів.

37. Поняття кодової відстані, перевіряючої та корегуючої здатності
38. Загальні принципи використання надлишковості при побудові корегуючих кодів. (В т.ч. приклади та геометрична модель)
39. Поняття кодової відстані. Зв'язок перевіряючих та корегуючих характеристик коду з кодовою відстанню.
40. Паритетне кодування. Паритетне кодування блоків даних.
41. Методи автоматичного виявлення помилок.
42. Коди Хемінга.
43. Циклічні коди. Загальні поняття та визначення. (Перехід від двійкового коду до многочленів, висновок та наслідок)
44. Основні принципи побудови циклічних кодів.
45. Формування циклічних кодів методом множення поліномів.
46. Формування циклічних кодів методом ділення поліномів.
47. Використання циклічних кодів для виявлення та корегування помилок.
48. Апаратні засоби формування циклічних кодів.

Рекомендована література

Основна

№	Назва	Режим доступу
1.	Ямненко Ю. С. Теорія інформації та обробка сигналів-1: конспект лекцій: навч. посіб. / Ю. С. Ямненко, К. С. Клен. – Київ: КПІ ім. Ігоря Сікорського, 2019. – 120 с.	https://core.ac.uk/reader/323535460
2.	Курко А. М. Введення в теорію інформації: посібник до вивчення дисципліни / А. М. Курко, В. Я. Решетник – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017. – 108 с.	https://core.ac.uk/reader/161261285
3.	Мережні інформаційні технології: навчальний посібник / О. А. Мясіщев, В. М. Джулій, С. Р. Красильников, В. М. Чешун. – Хмельницький: ХНУ, 2012. – 422 с.	Бібліотека ХНУ
4.	Романюк М. І. Основи теорії інформації та кодування. Конспект лекцій: навчальний посібник / М. І. Романюк, Ю. Г. Савченко; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2019. – 70 с.	https://core.ac.uk/reader/323526579
5.	Романюк М.І. Основи теорії інформації та кодування: лабораторний практикум: навчальний посібник / М.І. Романюк, Г.Г. Власюк; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 81 с.	https://ela.kpi.ua/bitstream/123456789/23943/1/Posib_LR_OTIK.pdf
6.	Бойко Ю. М. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад: монографія / Ю. М. Бойко, В. А. Дружинінін, С. В. Толюпа. - Київ: Логос, 2018. - 227 с.	http://elar.khnu.km.ua/jspui/handle/123456789/6291
7.	Кодування джерел інформації та каналів зв'язку: навчальний посібник / [Беркман Л.Н., Бондарчук А.П., Гайдур Г.І., Чумак Н.С.]. – Київ: ННІТІ ДУТ, 2018. – 91 с.	http://www.dut.edu.ua/ru/lib/1/category/1157/view/1619
8.	Бурячок В. Л. Основи інформаційної та кібернетичної безпеки: навчальний посібник. / В. Л. Бурячок, Р. В. Киричок, П. М. Складанний. – К., 2018. – 320 с.	http://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf
9.	Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д. т. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.	https://drive.google.com/file/d/1jACvCh2O4duJOYA3uLUID8cdVf2EFSWU/view?usp=sharing

Додаткова

10.	Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗІ НТУУ «КПІ», 2016. – 104 с.	https://core.ac.uk/reader/47235215
11.	Тарнавський, Ю. А. Технології захисту інформації: підручник / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.	https://core.ac.uk/reader/323530801
12.	Беркман Л.Н. Основні поняття та теореми теорії інформації: навчальний посібник для самостійної роботи студентів ВНЗ / Беркман Л.Н., Комарова Л.О., Чумак О.І. – Київ: ДУТ ННІТІ, 2015. – 91 с.	http://www.dut.edu.ua/ua/lib/1/category/1098/view/871
13.	Шинкарук О.М. Основи функціонування багатоканальних систем передачі інформації: навч. посіб./ О.М. Шинкарук, Ю.М. Бойко, І.І. Чесановський. – Хмельницький: ХНУ, 2011. – 245с.	Бібліотека ХНУ

14.	Основи теорії інформації та кодування: підручник. – 3-є вид., переробл. та доповн. / за ред. І.В. Кузьміна. – Хмельницький : ХНУ, 2009. – 373 с.	Бібліотека ХНУ
15.	Блинова И. В. Теория информации: учебное пособие / И. В. Блинова, И. Ю. Попов – СПб: Университет ИТМО, 2018. – 84 с.	http://mathdep.ifmo.ru/files/library/975.pdf
16.	Журавлева Л. М. Теория передачи сигналов: учебное пособие / Л. М. Журавлева. – М.: РУТ (МИИТ), 2017. – 149 с.	http://library.miit.ru/methodics/04022018/Журавлева%20Теория%20передачи%20сигналовА4.pdf
17.	Залюбовський В. С. Дослідження методів завадостійкого кодування інформації у цифрових системах передачі даних / Владислав Сергійович Залюбовський // Новітні інформаційні системи та технології. – Полтава: ПНТУ, 2015. – Т. (3). – Режим доступу: http://journals.nupp.edu.ua/mist/article/view/515 .	http://journals.nupp.edu.ua/mist/article/view/515
18.	Foundations of Coding Compression, Encryption, Error Correction / [Jean-Guillaume Dumas, Jean-Louis Roch, Eacuteric Tannier, Sébastien Varrette.]. – Hoboken, New Jersey : Published by John Wiley & Sons, Inc., 2015. – 512 p.	https://www.pdfdrive.com/foundations-of-coding-compression-encryption-error-correction-e200381644.html
19.	Ivaniš P. Ivaniš Information Theory and Coding - Solved Problems / Predrag Ivaniš, Dušan Drajić. – Cham, Switzerland : Springer International Publishing AG, 2017. – 517 p.	https://www.pdfdrive.com/information-theory-and-coding-solved-problems-e179623592.html
20.	Error-Correction Coding and Decoding: Bounds, Codes, Decoders, Analysis and Applications / [Martin Tomlinson, Cen Jung Tjhai, Marcel A. Ambroze, Mohammed Ahmed, Mubarak Jibril.]. – Cham, Switzerland : Springer, 2017. – 527 p.	https://www.pdfdrive.com/error-correction-coding-and-decoding-bounds-codes-decoders-analysis-and-applications-e158305925.html
21.	Письмак Д. О. Перешкодостійке кодування повідомлення електронного підпису. / Д. О. Письмак, В. П. Малайчук, С. В. Клименко. // Актуальні проблеми автоматизації та інформаційних технологій. – 2017. – Том 21. – С. 123-131.	https://www.readcube.com/articles/10.15421%2F431714
22.	Здробилко А. В. Завадостійке кодування в цифрових системах зв'язку / А. В. Здробилко, С. В. Денбновецький // Цифрові технології. – 2015. – Вип. 17. – С. 30-34.	http://nbuv.gov.ua/UJRN/c_t_2015_17_5
23.	Погребняк Л. М. Оцінка ефективності завадостійкого та просторового кодувань в нестационарних частотно-селективних каналах систем військового радіозв'язку / Л. М. Погребняк, М. І. Науменко. // Збірник наукових праць ВІТІ. – 2017. – № 4 –С. 103-110.	http://www.viti.edu.ua/files/bk/2017/4/14_4_2017.pdf
24.	Galić I. Image compression with B-tree coding algorithm enhanced by data modelling with Burrows-Wheeler transformation / Irena Galić, Časlav Livada, Branka Zovko-Cihlar. // Automatika: Journal for Control, Measurement, Electronics, Computing and Communications. – 2017. – Volume 57, Issue 1. – P. 76-88.	https://www.tandfonline.com/doi/pdf/10.7305/automatika.2016.07.282?needAccess=true
25.	An effective error correction scheme for arithmetic coding / Qiuzhen Lin, Kwok-Wo Wong, Ming Li, Jianyong Chen// Mathematical Problems in Engineering. – 2015. – Volume 2015. – P. 1-10.	http://downloads.hindawi.com/journals/mpe/2015/861093.pdf
26.	Magli E. Onboard payload data compression and processing for spaceborne imaging / Enrico Magli, Diego Valsesia, Raffaele Vitulli. // International Journal of Remote Sensing. – 2018. – Volume 39, Issue 7. – P. 1951-1952.	https://www.tandfonline.com/doi/pdf/10.1080/01431161.2017.1409483?needAccess=true
27.	Lake Bu New byte error correcting codes with simple decoding for reliable cache design / Lake Bu, Mark Karpovsky, Zhen Wang. //IEEE 21st International On-Line Testing Symposium (IOLTS). – 2015. – P. 200-205	https://sites.bu.edu/mark/files/2018/02/239.pdf

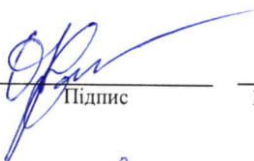
28.	Performance Study of BCH Error Correcting Codes Using the Bit Error Rate Term BER / Elghayyaty Mohamed, Hadjoudja Abdelkader, Omar Mouhib, El Habti El drissiAnas. // International Journal of Engineering Research and Applications (IJERA). – 2017. – Vol. 7, Issue 2 (Part -2) – P.52-54.	https://issuu.com/www.ijera.com/docs/j0702025254
29.	Das A. Low Complexity Burst Error Correcting Codes to Correct MBUs in SRAMs / Abhishek Das, Nur A Touba. // Proceedings of the 2018 on Great Lakes Symposium on VLSI. – 2018. – P. 219-224.	https://dl.acm.org/doi/pdf/10.1145/3194554.3194570
30.	Zero-Shot Action Recognition With Error-Correcting Output Codes / Jie Qin, Li Liu, Ling Shao, Fumin Shen, Bingbing Ni, Jiaxin Chen, Yunhong Wang. // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). – 2017. – P. 2833-2842.	https://openaccess.thecvf.com/content_cvpr_2017/papers/Qin_Zero-Shot_Action_Recognition_CVPR_2017_paper.pdf

Інформаційні ресурси

1. Модульне середовище для навчання MOODLE (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань) Доступ до ресурсу: <https://msn.khnu.km.ua>.

2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/plage_lib.php.

Розробник


Підпис

К.Т.Н., доцент
Вчений ступінь, звання

В.С. Орленко
Ініціали, прізвище

Погоджено

Гарант освітньої програми


Підпис

К.Т.Н., доцент
Вчений ступінь, звання

В.М. Чешун
Ініціали, прізвище

Зав. кафедри кібербезпеки та комп'ютерних систем і мереж


Підпис

К.Т.Н., доцент
Вчений ступінь, звання

Ю.П. Кльоц
Ініціали, прізвище